Defense Manpower Data Center

Personnel Security & Assurance

Joint Personnel Adjudication System (JPAS) Frequently Asked Questions (FAQs)

Document Version 4.5
23 December 2016

Table of Contents

Section 1: General Questions

1. What is the Joint Personnel Adjudication System (JPAS)?

- Serves as a master repository that performs comprehensive personnel security management of all DOD employees, military personnel, civilians and DOD contractors.
- Composed of two sub-systems:
  - Joint Adjudication Management System (JAMS) - Record eligibility determinations and unclassified investigation comments. Supports the adjudication process and automates security information records
  - Joint Clearance and Access Verification System (JCAVS) - Enables DoD Security Managers and officers the ability to view current eligibility information. It also provides the ability to update Personnel Security Information and security history

2. What are the software and hardware requirements for JPAS?

- Each JPAS user will be required to have a Web browser with128-bit security (SSL) encryption and a Public Key Infrastructure (PKI) certificate smartcard/token. Please see the JPAS PKI FAQs and DoD Approved PKI Providers on DMDC's JPAS website for further technical guidance on PKI certificates required to access JPAS.

3. How do I get a JPAS account?

- For detailed information on how to request a JPAS account, including clearance requirements, PKI certificates, mandatory training, and Letter of Appointment (LOA) requirements, refer to the JPAS Account Management Policy and the *Request a JPAS Account* link on the *JPAS Website*.
- Non-DoD/Other Federal Government agencies should utilize the Office of Personnel Management (OPM) Central Verification System (CVS) for personnel clearance eligibility verifications. The OPM CVS contains information on background investigations, credentialing determinations, suitability determinations, and security clearances. OPM CVS contains a data bridge to JPAS for clearance reciprocity purposes. Questions for access to the OPM CVS should be directed to OPM.

4. What are JCAVS user levels and clearance requirements?

- LEVEL 2 - Security personnel with TS SCI eligibility at unified command, DoD agency, military department or major command/equivalent headquarters. Clearance requirement for read and write access – SSBI (Tier 5).
- LEVEL 3 - Security personnel with TS SCI eligibility at echelons subordinate to Level 2 at a particular geographic location (installation, base, post, naval vessel). Clearance requirement for read and write Access-SSBI (Tier 5)
- LEVEL 4 - Security personnel with at least Interim Secret eligibility at unified command, DoD agency, military department or major command/equivalent headquarters. Clearance Requirement for read and write access - NACLC/ANACI (Tier 3)

- LEVEL 5 - Security personnel with at least Interim Secret eligibility at echelons subordinate to Level 4 at a particular geographic location (installation, base, post, naval vessel). Clearance requirement for read and write access - NACLC/ANACI (Tier 3)
- LEVEL 6 - Unit security manager (additional duty) with at least Interim Secret eligibility responsible for security functions as determined by responsible senior security official. Clearance requirement for read and write access - NACLC/ANACI (Tier 3)
- LEVEL 7 - Entry control personnel with at least Interim Secret eligibility. Individuals who grant access to installations, buildings, etc. Clearance requirement for read access - NACLC/ANACI (Tier 3)
- LEVEL 8 - Entry control personnel with TS SCI eligibility. Individuals who grant access to SCIF installations, buildings, etc. Clearance requirement for read access - SSBI (Tier 5)
- LEVEL 10 - Visitor Management with at least Interim Secret eligibility. Level 10 users will have the same view of the JCAVS Person Summary as a JCAVS Level 7 User. They will receive Visit Notifications when their SMO is being notified of a visit. A Level 10 User may not be an Account Manager, create or delete an account at any level.

5. Can I logon to JPAS using my boss, friend or co-worker's username/password or PKI certificate?

- It is a violation of DoD Regulations to share username/password, any approved active Public Key Infrastructure (PKI) hardware, or allow an individual to access another person's JPAS account or certificate in any manner or form. Only the authorized account and certificate holder is permitted to access/use his/her account. Examples of Approved Active PKI hardware include Common Access Cards (CAC) and Personal Identity Verification (PIV) cards, approved corporate badges, and External Certificate Authority (ECA) cards/tokens, among others.

6. How will DMDC communicate upcoming deployments, modifications, and information regarding JPAS?

- Users can find information on JPAS by going to the JPAS Welcome Screen within the JPAS application. The DMDC web page also provides alerts, notices, and user guide resources at https://www.dmdc.osd.mil/psawebdocs.

7. Who determines the access authorizations for JPAS?

- Each service/agency/company will determine the specific JPAS customer user base for their respective service/agency/company.

8. Who designates Account Managers? Are secret clearances necessary?

- Account Managers are designated by their service/agency/company. In JCAVS, Levels 4, 5, 6, 7 and 10 require at least Interim Secret eligibility. JCAVS levels, 2, 3 and 8 require a TS SCI. For JAMS at minimum a favorably adjudicated SSBI with a Top Secret eligibility is required.

9a. How do I get errors in the Personal Identification Data (PID) section corrected in JPAS?

- Errors in a person's Personally Identifiable Information (PII) data such as name, date of birth, or Social Security Number can be corrected through the DMDC Contact Center as long as you are not a Military or a DoD Civilian. If you are military or DoD Civilian, please contact your Personnel Support Detachment (PSD), Human Resources Office (HRO), or Personnel Center.

  It is possible for names, dates of birth and other PII to be overwritten in JPAS with outdated information from the Person Data Repository (PDR) or other data sources (e.g., service personnel centers) that feed JPAS. The JPAS Data Correction Checklist can assist users in determining how to correct PII in the proper database.

9b. I've noticed my employee PII information is getting overwritten each month. What can I do to make sure it doesn't happen again?

- Industry FSOs should monitor their employee records regularly to make sure PII is not overwritten by the PDR or any other data interface updates. If you discover the name or DOB is incorrect, the JPAS Data Correction Checklist can assist users in determining how to correct PII in the proper database.

10. What is the JPAS operational policy on printouts from JCAVS?

- Personnel are granted access to JPAS for the specific purpose of verifying eligibility and determining access to classified information of their service members/employees and/or visitors. There is no authorized use of JPAS printouts. Security Officers/Facility Security Officers should never print out any screen, screenshot, or provide JPAS printouts to any agency or person.

11. What are the plans to replace JPAS?

- As mandated by The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) and guided by relevant Executive Orders and GAO recommendations to deliver and maintain an appropriately vetted workforce, the DoD has begun to overhaul the security and suitability processes via the use of an enterprise-wide IT solution. Through a closely coordinated and phased approach, the Defense Information System for Security (DISS) will replace JPAS. Upon full implementation of the DISS family of systems, DoD will decommission JPAS (currently scheduled for November 2016).

Section 2: Application FAQs

12. Is there an indication that a save took place after I click Save?

- Currently, there is no indication that the save took place other than a browser screen refresh.

13. What happens when JPAS goes down in the middle of a user's session?

- You need to contact your Account Manager or the DMDC Contact Center to log you off or unlock your account.
- Alternately, you can wait 15 minutes until the system automatically terminates the session before attempting to re-authenticate.

14. What if I encounter a message that says, "Do you wish to allow the cookie to be set?" when trying to log in to the JPAS system?

- Your browser must have Cookies enabled in order to work with the JPAS system.
- To enable cookies with JPAS in Internet Explorer go to Tools → Internet Options → Privacy Tab, under the settings heading select the "Sites" button. In the prompt type https://*.dmdc.osd.mil and then click the "Allow" button, then OK and apply your changes.
- To enable cookies with JPAS in Firefox go to the Options menu → Privacy Tab → Under the "History" header if you see the dropdown that says "Firefox will: Remember history" you have already enabled cookies for all sites, if you only want to enable for JPAS specifically, or otherwise delimit what sites to accept cookies from click the drop down and select the "Use custom settings for history," option. Once selected more options will appear underneath, you will want to ensure the box associated with "accept cookies from sites:" is checked and then click the "exceptions" button. Here you can enter https://*.dmdc.osd.mil and then 'allow.'

15. In the PID Section, why is there an eligibility displayed but no investigation data displayed?

- When JPAS receives data from the CAFs, the eligibility is provided for the person and all of the investigations and adjudications that they have. They do not, however, match the eligibility to the specific investigation that supported it in the history.
- If you are reviewing legacy data and the investigation at the top of the screen is blank, look at the investigation summary at the bottom of the screen for the information needed.

16. While updating/maintaining my JPAS user profile, I received a JPAS Server Exception Encountered error message, how can I avoid this error?

- This error is generally a result of the input of multiple email addresses into that specific field.
- In order to avoid this error, ensure that only one email address is entered for that specific user (i.e., no additional emails for that user or other addresses for coworkers/team members).

17. I see that I can select a person using a DoD Identification Number (DoD ID), Last Name, and DOB value. What is DoD ID?

- This is the Department's unique identifier for every individual associated with the DoD.
- This initiative was implemented to help provide privacy assurances by minimizing the storage, use and transmission of individuals' SSNs.
- Previously users were able to select a person using a DoD ID only. The DoD Privacy Office requested that DMDC remove the EDI Search function as it was a violation of subjects' PII. As a result, DMDC worked with all Services for over 8 months to keep the EDI Search function in JPAS as the functionality was still needed. The compromise was to allow SOs/FSOs to continue using EDI Search but require Last Name and DOB values, much like the SII Search. The requirement to use Last Name and DOB values for EDI Search also eliminates a source of possible JPAS misuse.

18. What is e-QIP?

- The Electronic Questionnaire for Investigations Processing (e-QIP) has replaced the Electronic Personnel Security Questionnaire (EPSQ) as the automated request application for personnel security investigations and clearances within the Department of Defense (DoD).
- e-QIP is a secure website which will eventually contain all PSI forms, including the SF-86, SF-85P, and the SF 85. DoD security professionals can now initiate the request through the Joint Personnel Adjudication System (JPAS) which permits applicants to access the site and complete their personnel security questionnaires (PSQ) online.

19. Revised Federal Investigative Standards

- In December 2012, the Office of the Director of National Intelligence (ODNI) and Office of Personnel Management (OPM) jointly issued revised federal investigative standards on the conduct of background investigations for individuals that work for or on behalf of the federal government in order to bring consistency to investigative quality expectations.
- In early fiscal year 2016, the Tiers 1, 2, and 3 investigation types are being implemented as part of the phased approach for implementation of the Federal Investigative Standards. As a result, the investigation types of the National Agency Check and Inquiries (NACI) and Minimum Background Investigation (MBI) used for Suitability and Trustworthiness are replaced with Tier 1 and 2 types respectively, along with the National Agency Check with Law and Credit (NACLC) and Access National Agency Check with Written Inquiries + Credit Check (ANACI) are being replaced with the Tier 3 investigation when Confidential or Secret access to classified information is required.

- The Investigative Standards will change as outlined below:

Tiered Investigation Standards							
Why We Investigate	Public Trust			National Security			
Reason	Suitability			Access to Classified Information			
Position	Low-Risk	Moderate Risk	High Risk	Confidential	Secret	Top Secret	SCI
Position Sensitivity	Non-Sensitive			Non-Critical Sensitive		Critical Sensitive	Special Sensitive
Tiered Investigation Associated	Tier 1	Tier 2	Tier 4	Tier 3	Tier 3	Tier 5	Tier 5
Current Type Investigation	NACI	MBI	BI	NACLC/ANACI		SSBI	
Standard Form Used	SF-85	SF-85P		SF-86			
Who Submits	Government Agencies (not NISP contractors)			FSOs			

20. What are the timelines when initiating, reviewing and approving an e-QIP submission?

- Initiating
  - 30 Days: Once an Investigation Request is initiated in JPAS, an applicant has 30 days to login to e-QIP and start their Personnel Security Questionnaire (PSQ). If they do not login, the Investigation Request is terminated.
  - 90 Days: Once an Investigation Request is initiated in JPAS, an applicant has 90 days after their initial e-QIP login date to complete their PSQ. If they do not complete the PSQ, the Investigation Request is terminated.
- Reviewing and Approving
  - 90 Days: Once the applicant has completed the PSQ, it must be reviewed and approved by the appropriate agency within 90 days. If not, the Investigation Request is terminated.
- What are some other important e-QIP timelines?
  - Pending PSQs
    - 30 Days: An Investigation Request that remains in a Pending Status and is not "Initiated" will be deleted 30 days after creation.
  - Stopped PSQs
    - 90 Days: If an applicant has started to complete a PSQ but the Investigation Request is stopped, it must be resumed within 90 days.
    - 30 Days: If the applicant has not started to complete a PSQ, but the Investigation Request is stopped, it must be resumed within 30 days.
  - Revised PSQs
    - 60 Days: An applicant has 60 days to log into e-QIP and complete updates to their PSQ if revisions are required.
  - Facility Notifications
    - 15 Days: An Investigation Request must be ready to be reviewed 15 days after initiation for an active Person Category with Key Management Personnel (KMP) category classification in a Facility with a status of "In Process" or a Facility Notification will be generated.

21. How do I access e-QIP?

- http://www.opm.gov/e-qip
- The applicant's Security Officer must have first initiated the Investigation Request.
- A JPAS user must have a JCAVS user level 2 through 6 with the appropriate Investigation Request permission in order to initiate an investigation request. See FAQ question #3 in General Questions section of this document.

22. Can I view the applicant's personnel security questionnaire through JPAS?

- Yes, if you have Review or Approve permissions granted on your JCAVS user level.

23. How should Release Forms and Fingerprint Cards be submitted and where does the FSO send them?

- Fingerprint cards and Release forms must be forwarded to the Office of Personnel Management (OPM), the investigative provider for the DoD. It is critical to use the release form generated during the applicant's printing of the questionnaire as there is a code on the form that assists OPM with matching the release to the questionnaire. OPM must receive fingerprint cards and releases within 14 days of receipt of the approved investigation request. Fingerprint cards and releases should be forwarded via:
  - E-mail scanned signature and release forms, Livescan Fingerprints to: e-Qip.attachments@opm.gov
  - Fax Release forms (without fingerprint cards) to: 724 794-1412 (Attn: e-QIP Release Forms Processor).

24. Can I use the click-to-sign functionality to sign my e-QIP documents?

- Although the click-to-sign feature is available when users directly log in to e-QIP, OPM has confirmed it is not available to JPAS users (Accessions or non-Accessions) through the JPAS/e-QIP interface.

25. If JPAS reflects an eligibility of Denied or Revoked, may I submit a request for investigation?

- Only if the revocation dates is older than 12 months (one year) from the current date. A person whose eligibility is denied or revoked must wait one year before they can reapply.
- For other relevant adjudicative and eligibility inquires please refer to the DoD CAF website

26. If JPAS reflects an eligibility of Action Pending, may a new request be initiated?

- No. The pending action must first be completed or resolved.

27. How do I update an investigation from an NAC (Tier 1) to NACLC/NLC (Tier 3) to gain access to JPAS?

- The company FSO will need to resubmit a SF86 to the DOD CAF. In the remark section, indicate "Please upgrade investigation to meet JPAS access requirements.

28. If a contractor needs access to JPAS, what do they do if the person has a NLC with Confidential eligibility?

- The security manager should submit a RRU in JPAS indicating that the person needs a secret eligibility for access to JPAS.

29. If a Nondisclosure Agreement (NDA) date is different in JPAS than what I have on file, should I change this date?

- If the NDA date displayed in JPAS is earlier than the date on file, do not change it.
- Note: The NDA only needs to be signed once and is valid for the lifetime of the clearance.

30. What is eligibility "Loss of Jurisdiction" and who do I contact when an individual has an eligibility of "Loss of Jurisdiction"?

- A "Loss of Jurisdiction" is when a subject has terminated/separated or retired and the CAF no longer has the authority to make any additional investigative/adjudicative decisions regarding the eligibility.

31. What happens if one of my subjects in JPAS has had their eligibility changed to either a generic “Favorable” or “Eligibility Administratively Withdrawn”?

- As a result of several Data Quality Initiatives (DQIs), select subjects may have their eligibility changed to a “Favorable” or “Eligibility Administratively Withdrawn” status. These new eligibility statuses do not reflect adverse info placed on the subject, but rather are part of DQIs targeted to improve JPAS data.

32. Should I update the Marital Status to reflect ‘Married’ for a same sex marriage?

- Yes, the DoD recognizes same-sex marriages. Therefore, a subject’s marital status can be updated to reflect ‘Married’ if the subject is married to a same-sex or opposite sex spouse. The same procedures would apply.

33. Should I use the security incident process to report subjects who are eligible and have used or possess marijuana?

- Yes, even though use and/or possession of marijuana has been legalized or decriminalized in certain states, it remains a schedule 1 narcotic as defined by the Drug Enforcement Agency (DEA) and the Department of Justice. As such use or possession can be litigated on the Federal level under the Controlled Substances Act (CFR Title 21). All substance abuse issues (to include alcohol) are relevant to Federal Personnel Security determinations and should be reported appropriately.
- This relevance to national security determinations was confirmed by Director of National Intelligence (DNI) Memo ES 2014-00674

Section 3: JPAS Reports

34. Why do I see a blank screen pop up when I initiate a report for immediate delivery?

- Upon initiating a report, users will see a pop up box stating that the requested report is loading and a blank screen will appear. DO NOT CLOSE THE BLANK SCREEN, and no not hit the back button in the browser; your report is being processed. Wait for the loading icon to appear, which may take between 30 seconds and one minute, depending on the report and parameters selected.

35. How do I convert a Comma Separated Values (.CSV) file into an Excel spreadsheet?

- If the desired report has the .CSV option, refer to applicable section below (depending on Excel version) for instructions on how to import a .CSV or .TXT file into Excel.
  1. From the Office Ribbon: Select Data, Get External Data, From Text.
  2. Navigate and select the file to import (make sure "Files of type: " is listed as "All Data Sources").
  3. A prompt will be displayed – leave "Delimited" selected. Click Next.
  4. On "Delimiters", select "Comma".
  5. Click Finish.

36. Considering the timeout policy, will my connection with JPAS timeout while I am running reports?

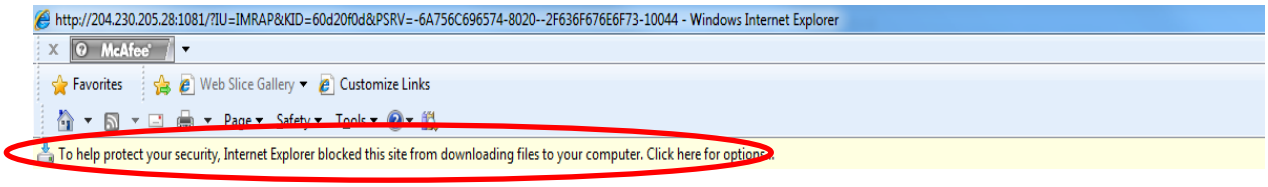
- If the user continues to work in JPAS while they are running reports, they will not timeout of the application.
- Depending on the size of the report, it can take a long time to process and render. Internet Explorer does have a default 60 minute timeout that is organic to the browser. If the report is large enough, it is recommended that the user run the report in the background and pickup mode, and not in the immediate mode. It will queue up in the cache, and the user can go back into JPAS and download the report when it completes.

37. How do I convert an Excel spreadsheet into a PDF file?

- If you are using Microsoft Office 2010, follow these directions:
  1. Open the selected spreadsheet in Excel 2010.
  2. Click on the File Menu.
  3. Click on Save & Send.
  4. Click on Create PDF/XPS Document under File Types.
  5. Click on the Create PDF/XPS Icon.
  6. Ensure .PDF file type is selected.
  7. Click on Publish and save the document.
- If using a program than Microsoft Office or an earlier version, please read the following guidance:
  1. In order to save a file as a .pdf file you will need to have a PDF writer installed on your computer.
  2. To verify you have a PDF Printer/Creator installed open the location that displays all installed Printing devices (Printers, Faxes, etc.) and verify there is an option for PDF.
  3. For Microsoft Windows, these applications are listed under Devices and Printers which can be selected by clicking on the Windows Icon usually found in the bottom left corner of the screen and selecting Devices and Printers from the menu of program options.
  4. If you do not have such a device installed, conduct an Internet search for "print pdf" or "free print pdf" to obtain a program or consult with your IT department for further guidance.
- Note: The JPAS reports server is capable of returning a report in PDF format, you can just select that option when generating a new report

38. I am using Internet Explorer and my report is not displaying, how do I correct this?

- Newer versions of Internet Explorer have a security feature that requires a user to perform a verification step in order to display data. Unfortunately this action will be required to be completed each time a report is generated. If you do not see your report and are using Internet Explorer, look for the yellow bar in Internet Explorer (circled in red below). Click the yellow bar and you will see a list of options. Select "Download File" and then select "Open" to see your report.
- Users can also change the default setting for automatic file downloads by going to Tools → Internet Options → Security Tab → Zone → Custom Level → File Download and switching the toggle from disable to enable.



39. Whom do I contact regarding technical support for reports?

- If you experience problems with JPAS reports, please see the guidance above regarding blank pop up screens, report formats and problems with Internet Explorer not rendering reports in this section. If you continue to experience problems with processing reports, please contact the DMDC Contact Center.

Section 4: JPAS Security Incidents and System Misuses

40. What are the most common misuses of JPAS?

- There are several different types of JPAS misuses that can occur. Below is a list of the most common misuses of JPAS, which are not limited to:
  - Sharing of username, password, CAC/PIV/other DoD approved authentication mechanism and/or associated PIN numbers to access the system
  - Allowing non-cleared/unauthorized individuals to access the system
  - Leaving the JPAS application unsecure while logged in
  - Allowing others to view data on the JPAS screen that do not have the proper authorization
  - Printing or taking a screenshot of JPAS data
  - Querying the JPAS application for 'celebrity' records
  - Querying the JPAS application for your own record
  - Entering or otherwise using test or "dummy" SSNs in JPAS
  - Knowingly entering false or inaccurate information into the system
  - Initiating investigations for subjects who you have no owning/servicing relationship, or are otherwise not appropriately sponsored for a clearance.
  - Taking any action on your own record (e.g., submitting visit requests, attempting to indoctrinate, establish an owning/servicing relationship of yourself, etc.)
  - Querying the JPAS application for information or records you have no need to know and/or authority to view to conduct your official duties.
  - Querying the JPAS application for records or persons no longer affiliated with your Security Management Office or the Department of Defense.
- When selecting the "Agree" option on the JPAS disclosure page prior to logging onto the system, users are agreeing to all relevant DoD Information Assurance regulations, the Privacy Act of 1974, and the JPAS Account Management Policy.

41. What do I do if I witness a misuse of JPAS?

Please call the DMDC Contact Center (800-467-5526) to report any potential misuses of JPAS you may have observed.

42. What happens in the event of an alleged JPAS misuse?

- As the Cognizant Security Agent (CSA) for JPAS, when DMDC is made aware of an alleged misuse of JPAS, the system must be protected from loss of data confidentiality, integrity, and availability. As a result, the user(s) account(s) are administratively locked

and placed in administrative review, preventing any access to JPAS during the review. This practice limits risk to the system and its data. During an administrative review:

- The alleged will receive an Incident Notification Letter and any JPAS accounts connected to the incident are locked.
- Once the relevant data surrounding the incident is gathered, the JPAS Program Manager (along with government counsel when necessary) make a determination as to whether or not the incident occurred:
    i. If it is determined that the incident occurred, the user may have their account terminated and be permanently barred from receiving another JPAS (or future replacement system) account. A misuse of technology security incident will also be placed on the user's JPAS record for the DoD CAF to adjudicate.
    ii. If it is determined that the incident did not take place the user account may be unlocked.
- When an administrative review is complete, the user will receive an Outcome Notification Letter, outlining the decision and any subsequent actions.

43. I have received a JPAS incident notification letter, what should I do?

- Follow all instructions as outlined in the incident notification letter.
- If a user receives a JPAS incident notification letter, they may choose to directly respond with a personal statement addressing the incident.
- Note that the user(s) account(s) under administrative review will not be accessible, so please make appropriate coordination with other FSOs/AFSOs/SOs in your organization regarding your JPAS workload/tasks.
- All communication regarding a JPAS incident and/or administrative review should be directed to the email address provided in the notification letter.

44. What happens to my account in the event of an administrative review?

- In order to protect the confidentiality, integrity, and availability of the data in JPAS, the user's account will be locked and will not be accessible during the entire period of the administrative review.
    - In the rare circumstance where the integrity of an entire cleared organization/SMO is in question, all associated JPAS user accounts may be locked.
    - Appropriate investigative agencies may also be informed (e.g. Defense Criminal Investigative Service (DCIS), DoD Inspector General (DoDIG), etc.) dependent on circumstances and severity of the alleged incident.
- JPAS audit logs are reviewed by program leadership to determine exactly what actions were performed/taken by the subject inside of the system, to include every screen viewed and every action taken in JPAS.
- Note that your account will not be deleted/removed *due to inactivity* during an administrative review.

45. How long do administrative reviews take to complete?

- Administrative reviews have no defined timeframe. Factors such as the severity of the misuse, the number of individuals involved, third party investigations/input, government counsel involvement, and size of audit files, among other factors can all vary from incident to incident.

46. What are the potential consequences related to a misuse of JPAS, and is there an appeals process?

- If it is determined that a misuse has occurred the user is at risk of losing their JPAS account as well as being barred from reapplying for a JPAS account (to include future JPAS replacement systems) **PERMANENTLY.**
- A misuse of technology incident will be placed on the user's JPAS record for eventual adjudication by the CAF.
- An appeals process does exist; however, **only new and relevant evidence** may be presented to be considered for an appeal.